is stored on at least one storage device. The method includes decrypting a value required to decrypt the information. The value is decrypted by correctly solving an access formula describing a function of groups. Each group includes a list of at least one client. A requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula.

The Examiner rejected claim 1 with the following argument:

> As per claim 1, Carter illustrates a method for secure handling of information comprising: authenticating a user group with a user group identifier and corresponding password (see column 8, lines 51-59; figure 2, item 48; column 16, lines 16-29; and figure 9, step 152); as a result of authentication, obtaining the private key of the user (see column 16, lines 30-37 and figure 9, step 154); and using the private key to decrypt the encrypted document key that is required to decrypt the document (see column 16, lines 60-65 and figure 9, step 160).

Nowhere does the examiner mention an access formula. Further, none of the passages cited by the Examiner appear to relate to an access formula. The Examiner has thus failed to show that Carter teaches each element of Applicants' claim 1. Claim 2 depends from claim 1 and is therefore also patentable.

The Examiner rejected independent claim 9 as anticipated by Carter. Claim 9 provides a system for the secure handling of information stored on at least one untrusted storage device connected to a network. The system includes a key manager, at least one group server and at least one producer client. The key manager generates private key and public key matched pairs for use with an asymmetric encryption and decryption scheme. This scheme allows a file encrypted with a public key to be decrypted only with a matched private key. Each group server maintains at least one group. Each group has a list of client members allowed access to information produced by any client member of the group. The group server obtains a private key and matched public key for each group. Each producer client encrypts an information set to produce a data set based on an encryption value. An access formula is determined which expresses a logical combination of the at least one group for which access to the information set will be granted. A solution of the access formula by at least one solution group indicates that a client belonging to the at least one solution group may access the encrypted information set. The encryption value is asymmetrically encrypted using the determined access formula and the public key for each of the at least one group for which

access to the information set may be granted. The encrypted encryption value and the access formula are added to the data set and the data set is stored on at least one untrusted storage device.

The Examiner rejected claim 9 with a long paragraph that never mentions access formula, group server, producer client or many of the other terms used in claim 9. It is therefore virtually impossible to interpret the Examiner's rejection. In addition, the passages cited by the Examiner once again fail to provide any mention of an access formula in any of the cited passages or figures. Further, there appears to be nothing similar to Applicants' access formula contained in these passages. The Examiner has thus failed to show that Carter teaches each element of Applicants' claim 9. Claims 10-17 depend from claim 9 and is therefore also patentable.

The Examiner rejected claim 3 as obvious over Carter in view of Feistel. Claim 3 provides a method for the secure handling of information by at least one client using at least one untrusted storage device. Each client is connected to the at least one untrusted storage device using a network. The network has a key manager for issuing private key and public key matched pairs for use with an asymmetric encryption and decryption scheme, the scheme allowing a file encrypted with a public key to be decrypted only with a matched private key. The method includes creating at least one group having a list of at least one consumer client. A public key and a matched private key is acquired for each group. An information set is encrypted to produce a data set, the encryption based on a randomly generated number. An access formula is determined expressing logical combination of the at least one group for which access to the information set will be granted. Solution of the access formula by at least one solution group indicates that a consumer client belonging to the at least one solution group may access the encrypted information set. The randomly generated number is asymmetrically encrypted using the determined access formula and the public key for each of the at least one group granted access to the information set. The encrypted randomly generated number is added to the data set and the data set is stored on at least one untrusted storage device.

The Examiner indicated that Carter disclosed each element of claim 3 except for generation of a "random key." However, Carted does not disclose Applicants' access formula "expressing logical combination of the at least one group for which access to the information

set will be granted." No portion of Carter cited by the Examiner appears to relate in any manner to any kind of a formula, let alone Applicants' access formula.

The Examiner seems to assert that "arranging collaborative group identification" somehow relates to Applicant's step of "determining an access formula expressing logical combination of the at least one group for which access to the information set will be granted, solution of the access formula by at least one solution group indicating that a consumer client belonging to the at least one solution group may access the encrypted information set." The only passage cited by the Examiner to support this assertion is column 13, lines 18-28, which is reproduced as follows:

> During an identifying step 114, a collaborative group is identified by identifying one or more members of the group. Identification is accomplished by obtaining user identifiers 48 through dialog boxes or other interactive user interfaces, by identifying a group object 70 or other group identifier that is known to the operating system 46, or by other identification means familiar to those of skill in the art. In one embodiment, a default mechanism is employed whereby the user presently directing the collaborative access controller 44 is automatically identified as a member of the collaborative group.

This passage appears to refer to forming a group of members. This is not Applicant's access formula of claim 3, which is a logical combination of groups.

The Examiner has failed to establish a *prima facie* case of obviousness with regards to claim 3. Claims 4-8 depend from claim 3 and are therefore also patentable.

Claims 1-17 are pending in this application. These claims meet all substantive requirements for patentability. Applicants therefore respectfully request issuance of a patent. No fees are believed to be due by filing this paper. However, any fee incurred may be drawn from Deposit Account No. 19-4545 as specified in the Application Transmittal.

The Examiner is invited to telephone the undersigned to discuss any aspect of this case.

Respectfully submitted,

JAMES P. HUGHES

By _____
Mark D. Chuey, Ph.D.
Reg. No. 42,415
Attorney/Agent for Applicant

Date: July 1, 2002

BROOKS & KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
Phone: 248-358-4400
Fax: 248-358-3351